

IN THE CLAIMS:

Please substitute the following claims for the same-numbered claims in the application:

1-17. (Canceled).

18. (Currently Amended) A method for normalization of traffic data ~~in a network~~, received from an internet and transmitted to a local network, said method comprising:

dynamically establishing and maintaining a normalization table in a traffic normalizer, said traffic normalizer being interposed between said internet and said local network;

receiving a packet ~~of data~~ fragment from said internet at said traffic normalizer, said packet fragment being addressed to an end-system in said ~~network and comprising a fragment of a datagram~~ local network;

determining if an entry ~~is already contained~~ exists in said normalization table for said ~~datagram because of earlier received fragments~~ packet fragment, said entry including an identifier comprising identifying information from IDENTIFICATION, PROTOCOL, SOURCE IP ADDRESS, and DESTINATION IP ADDRESS header fields of said packet fragment;

if said entry ~~is already contained~~ exists in said normalization table, determining if ~~any conflicts exist~~ a conflict exists between said ~~fragment~~ entry and ~~said earlier received fragments a~~ prior entry;

if ~~[[a]]~~ said conflict exists, discarding said packet fragment; and

if said ~~conflicts do~~ conflict does not exist, simultaneously transferring said packet ~~of said~~

~~data fragment~~ to a network intrusion detection system and said end-system of said local network.

19. (Currently Amended) The method according to claim 18, all the limitations of which are incorporated herein by reference, ~~further comprising establishing information about said packet of said data without storing said data in said normalization table by extracting a header and calculating a length of said fragment.~~ wherein said entry further includes information from IDENTIFICATION, FLAGS, and FRAGMENT OFFSET header fields of said packet fragment, said information allowing calculation of a length of said packet fragment.

20. (Currently Amended) The method according to claim ~~18~~ 19, all the limitations of which are incorporated herein by reference, ~~further comprising recording wherein~~ partial and complete receipt of ~~said datagram~~ a packet, comprising two or more packet fragments, is signaled by a sliding bit-mask which that is moved to an offset, until said offset indicates receipt of all data of said datagram wherein said receipt of said datagram is cleared after a time period which is selected equal or slightly higher than a lifetime of the last fragment of said datagram is received packet.

21. (Currently Amended) The method according to ~~one of the claims 18~~ claim 20, all the limitations of which are incorporated herein by reference, wherein said entry further includes information corresponding to at least one of a distance pre-calculated TIME TO LIVE and a path Maximum Transfer Unit (MTU) to said end-system in said network that is monitored by said

~~network intrusion detection system is measured and stored in said normalization table one of~~
~~before said receiving and upon said receiving of said packet of said data addressed to said end-~~
~~system local network.~~

22. (Currently Amended) The method according to claim ~~18~~ 21, all the limitations of which
are incorporated herein by reference, ~~further comprising retrieving from said normalization table~~
~~TIME TO LIVE value for said packet of said data and measuring a path MTU for said end system,~~
wherein:

when ~~a contents of~~ said pre-calculated TIME TO LIVE ~~value~~ is ~~lower~~ less than a
predetermined value, then said pre-calculated TIME TO LIVE ~~value~~ replaces said predetermined
value; and

~~wherein~~ when said path MTU is ~~lower~~ less than a ~~size of the data~~ length of said packet, a
do not fragment FLAG is cleared.

23. (Currently Amended) A The method for ~~normalization of traffic data in a network~~
~~comprising:~~

~~dynamically establishing and maintaining a normalization table;~~
~~receiving a packet of data addressed to an end system in said network and comprising a~~
~~fragment of a datagram;~~
~~determining if an entry is already contained in said normalization table for said datagram~~
~~because of earlier received fragments;~~

~~if said entry is already contained in said normalization table, determining if any conflicts exist between said fragment and said earlier received fragments;~~

~~if a conflict exists, discarding said fragment; and~~

~~if said conflicts do not exist, simultaneously transferring said packet of said data to a network intrusion detection system and said end system; according to claim 18, all the limitations of which are incorporated herein by reference, wherein;~~

~~said dynamically establishing and maintaining comprises adding an aging bit to all entries in said normalization table, wherein said entry; and~~

~~said aging bit is set whenever said ~~entries are~~ entry is retrieved from said normalization table.~~

24. (Currently Amended) The method of according to claim 23, all the limitations of which are incorporated herein by reference, wherein said dynamically establishing and maintaining further comprises ~~periodically sequentially~~ resetting said aging ~~bits of all of said entries~~ bit after a first period and deleting ~~any of said entries~~ said entry with a previously set or reset aging ~~bits~~ bit.

25. (Currently Amended) The method according to claim 24, all the limitations of which are incorporated herein by reference, wherein said dynamically establishing and maintaining further comprises ~~periodically sequentially probing~~ determining, after a second time period, at least one of a ~~distance~~ pre-calculated TIME TO LIVE and a path MTU to ~~any end systems corresponding to any entries in said normalization table~~ said end system and updating said ~~normalization table~~

~~when said distance and said path MTU have changed~~ entry.

26-29. (Canceled).

30. (Currently Amended) A method for normalization of traffic data ~~in a network~~, received from an internet and transmitted to a local network, said method comprising:

dynamically establishing and maintaining a normalization table in a traffic normalizer, said traffic normalizer being interposed between said internet and said local network;

receiving a packet ~~of data~~ fragment from said internet at said traffic normalizer, said packet fragment being addressed to an end-system in said network and comprising a fragment of a datagram local network;

determining if an entry ~~is already contained~~ exists in said normalization table for said ~~datagram because of earlier received fragments~~ packet fragment, said entry including an identifier comprising identifying information from IDENTIFICATION, PROTOCOL, SOURCE IP ADDRESS, and DESTINATION IP ADDRESS header fields of said packet fragment;

if said entry ~~is already contained~~ exists in said normalization table, determining if ~~any conflicts exist~~ a conflict exists between said ~~fragment entry~~ entry and ~~said earlier received fragments~~ a prior entry;

if ~~[[a]]~~ said conflict exists, discarding said packet fragment;

if said ~~conflicts do~~ conflict does not exist, determining if a length of said packet fragment based on information from IDENTIFICATION, FLAGS, and FRAGMENT OFFSET header fields of

said packet fragment, fits a sliding bit-mask;

if said packet fragment does not fit said sliding bit-mask, redirecting said packet fragment; and

if said packet fragment does fit said sliding bit-mask, simultaneously transferring said packet ~~of said data~~ fragment to a network intrusion detection system and said end-system of said local network.

31-33. (Canceled).

34. (Currently Amended) The method according to claim 30, all the limitations of which are incorporated herein by reference, further comprising recording wherein partial and complete receipt of ~~said datagram~~ a packet, comprising two or more packet fragments, is signaled by a sliding bit-mask ~~which~~ that is moved to an offset, until said offset indicates receipt of all data of said ~~datagram wherein said receipt of said datagram is cleared after a time period which is selected equal or slightly higher than a lifetime of the last fragment of said datagram is received~~ packet.

35. (Currently Amended) The method according to ~~one of the claims 18~~ claim 34, all the limitations of which are incorporated herein by reference, wherein said entry further includes information corresponding to at least one of a ~~distance~~ pre-calculated TIME TO LIVE and a path Maximum Transfer Unit (MTU) to said end-system in said ~~network that is monitored by said~~

~~network intrusion detection system is measured and stored in said normalization table one of~~
~~before said receiving and upon said receiving of said packet of said data addressed to said end-~~
~~system~~ local network.

36. (Currently Amended) The method according to claim ~~48~~ 35, all the limitations of which are incorporated herein by reference, ~~further comprising retrieving from said normalization table TIME TO LIVE value for said packet of said data and measuring a path MTU for said end system,~~ wherein:

when a ~~contents of~~ said pre-calculated TIME TO LIVE ~~value~~ is ~~lower~~ less than a predetermined value, then said pre-calculated TIME TO LIVE ~~value~~ replaces said predetermined value; and

~~wherein~~ when said path MTU is ~~lower~~ less than a ~~size of the data~~ length of said packet, a do not fragment FLAG is cleared.

37. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by said machine to perform a method for normalization of traffic data ~~in a network~~, received from an internet and transmitted to a local network, said method comprising:

dynamically establishing and maintaining a normalization table in a traffic normalizer, said traffic normalizer being interposed between said internet and said local network;

receiving a packet ~~of data~~ fragment from said internet at said traffic normalizer, said

packet fragment being addressed to an end-system in said network and comprising a fragment of a datagram local network;

determining if an entry ~~is already contained~~ exists in said normalization table for said ~~datagram because of earlier received fragments~~ packet fragment, said entry including an identifier comprising identifying information from IDENTIFICATION, PROTOCOL, SOURCE IP ADDRESS, and DESTINATION IP ADDRESS header fields of said packet fragment;

if said entry ~~is already contained~~ exists in said normalization table, determining if ~~any conflicts exist~~ a conflict exists between said ~~fragment entry~~ entry and ~~said earlier received fragments a~~ prior entry;

if ~~[[a]]~~ said conflict exists, discarding said packet fragment; and

if said ~~conflicts do~~ conflict does not exist, simultaneously transferring said packet ~~of said data fragment~~ to a network intrusion detection system and said end-system of said local network.

38. (Currently Amended) The program storage device according to claim 37, all the limitations of which are incorporated herein by reference, wherein;

said dynamically establishing and maintaining comprises adding an aging bit to ~~all entries in said normalization table, wherein~~ said entry; and

said aging bit is set whenever said ~~entries are~~ entry is retrieved from said normalization table.